NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

# IT WORKFORCE ASSESSMENT FOR CYBERSECURITY (ITWAC)

## SUMMARY REPORT

# IT Workforce Assessment for Cybersecurity

The U.S. Department of Homeland Security (DHS), in partnership with the Federal CIO Council, developed and implemented the IT Workforce Assessment for Cybersecurity (ITWAC) to understand the composition and capabilities of the federal IT workforce executing cybersecurity responsibilities.

## Target Audience

- Federal civilian employees with IT-related responsibilities, regardless of occupational series

## Assessment Objectives

- Help agencies examine their cybersecurity workforce using the National Cybersecurity Workforce Framework
- Collect data to inform the National Initiative for Cybersecurity Education (NICE) efforts to support education, development, and maintenance of the Nation's cybersecurity workforce

## Assessment Timeframe

- Available from October 22 - November 16, 2012 (January 15- 31, 2013 for DoD)

# ITWAC Participation

- Over **80 agencies** were invited to participate in the assessment.
- Points of contact (POCs) were established in nearly every agency to raise awareness and communicate information regarding the assessment.
- Over **200,000** federal civilian employees were emailed the assessment.
- Over **32,700** individuals started the assessment.
- **22,956** IT professionals from **52** federal departments and agencies completed the assessment.
- The highest participation rates were as follows:

| Department/Agency | # Completed | % Completed |
|---|---|---|
| Department of Homeland Security | 8,208 | 35.76% |
| Department of Agriculture | 3,141 | 13.68% |
| Department of Navy | 2,612 | 11.38% |
| Department of Defense (HQ) | 1,856 | 8.09% |
| Department of the Army | 1,509 | 6.57% |

# ITWAC Findings – Composition

The following ITWAC participants demographic data provides a snapshot of the current composition of the cybersecurity workforce.

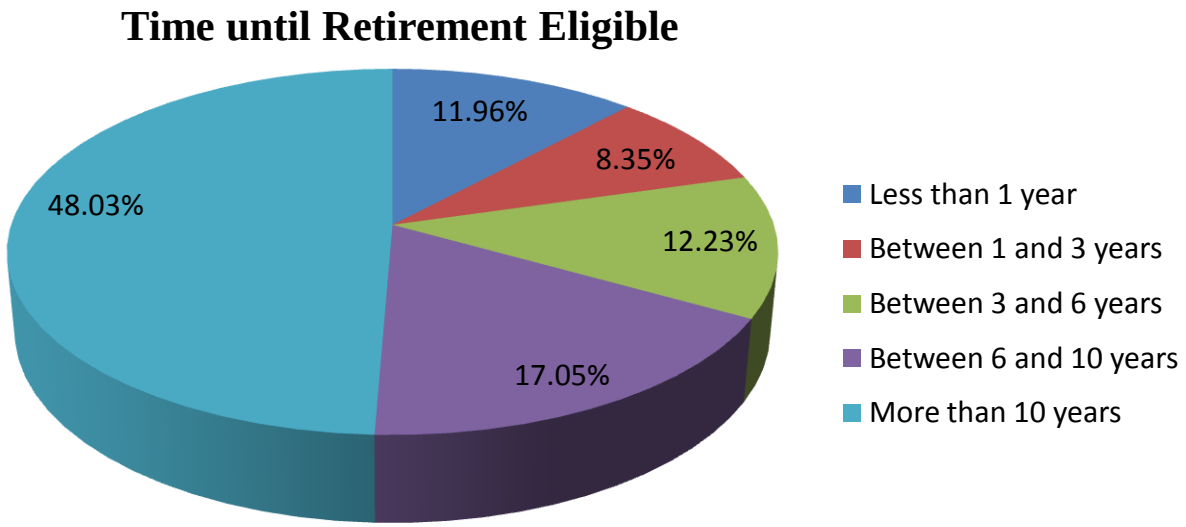
- GS 11-13 range accounted for the largest percentage of assessment participants (60.98%).
- The 25 and under age range had the lowest number of participants (0.96% of age responses).
- The GS 2210 - Information Technology Management occupational series with the largest percentage of participants (30.48%), followed by 1801 - General Inspection, Investigation, Enforcement, and Compliance (11.71%).
- Within the GS 2210 series, the Parenthetical Titles with the largest percentage of 2210 participants are displayed below:

| Parenthetical Title | Number of Participants | Percentage of 2210 Occupational Series | Percentage of Total Population |
|---|---|---|---|
| **Security** | 1,277 | 18.25% | 5.56% |
| **Customer Support** | 817 | 11.68% | 3.56% |
| **Systems Administration** | 777 | 11.10% | 3.38% |
| **Applications Software** | 730 | 10.43% | 3.18% |

# Retirement Eligibility Findings

Basic participant information provided a clearer picture of the retirement eligibility.

- Majority of the participants are above the age of 40 (78.50%)*.
- 11,026 participants (49.36% of the retirement eligibility response population) have 10+ years left before reaching retirement eligibility. However, 2,672 (11.96%) are eligible for retirement within the year.




*There may be cause for concern regarding the current and future pipeline of cybersecurity professionals. Without a younger cybersecurity workforce available to fill the ranks of retiring employees, it is possible the government will experience a significant manpower shortage.

# ITWAC Findings – Capabilities

The following slides provide a snapshot of the current capabilities of the cybersecurity workforce by analyzing:

- **Time Spent**: the amount of time participants currently spend in each Specialty Area.

- **Competency Proficiency**:
  - Current: participant self-assessment of proficiency in each Specialty Area.
  - Optimal: optimal proficiency rating in each Specialty Area for current role.

- **Training Needed**: Participants indicated the Specialty Areas where they believe additional training could benefit them in their current role.

# TIME SPENT FINDINGS

Time Spent in Specialty Areas was analyzed to better understand how the workforce is spending its time performing cybersecurity work.

- The total participant population indicated that they spend the majority of their time in work *other* than the Specialty Areas (53.81%).
- Largest percentage of time is spent in **Customer Service and Technical Support** Specialty Area (6.40%), followed by **Information Assurance (IA) Compliance** (3.91%).

Time Spent - Occupational Series:

- Participants in the 2210 - Information Technology Management series spends their most time in the 31 Specialty Areas (79.81%) and has higher percentages of Advanced or Expert proficiency.
- Participants in the 1550 - Computer Science series spends 70.07% of their time engaging in work related to the Specialty Areas.
- Participants in the 1811 - Criminal Investigation series spends, on average, 26.48% of their time in the **Investigation** Specialty Area.

# PROFICIENCY FINDINGS

For each Specialty Area, participants provided a self-assessment of current and optimal proficiency for their current role.

- **Customer Service and Technical Support** was the Specialty Area with the most ITWAC participants (73.90%) meeting or exceeding optimal proficiency.
- **Education and Training** has the next highest percentage of participants meeting or exceeding optimal proficiency (66.57%) followed by **Systems Development** (66.39%) and **Systems Requirements and Planning** (66.29%).
- Highest average Specialty Area proficiency ratings are displayed below:

| Specialty Area | Average Current Proficiency |
|---|---|
| Customer Service and Technical Support | 2.39 |
| Systems Requirements Planning | 2.28 |
| Test and Evaluation | 2.17 |
| System Administration | 2.14 |
| Systems Development | 2.13 |

# PROFICIENCY FINDINGS (CONT.)

Participant proficiency ratings were also analyzed to determine the Specialty Areas with the highest percentage of Advanced/Expert proficiency ratings.

- **Customer Service and Technical Support** Specialty Area accounted for the highest percentage of participants with either Advanced or Expert proficiency (26.82% of the population), followed by **Systems Requirements Planning** (24.26%).
- Specialty Areas with the lowest percentage of participants with Advanced or Expert proficiency were **Cyber Operations** (5.67%), **Threat Analysis** (6.03%) and **Targets** (6.04%).

| Occupational Series | Specialty Area | Advanced/Expert Proficiency (%) |
|---|---|---|
| 2210 | Customer Service & Technical Support | 58.85% |
| 1550 | Systems Requirements Planning | 41.47% |
| 1811 | Investigation | 38.63% |
| 0855 | Test & Evaluation | 30.46% |

# Training Findings

Participants also indicated the Specialty Areas where they believe additional training could benefit them in their current role.

- Training needs were found across the board in **Information Assurance (IA) Compliance** and **Vulnerability Assessment and Management.** The table below displays the Specialty Areas with the greatest training need according to participants:

| Specialty Area | Participants indicating Training Needs (%) |
|---|---|
| Information Assurance (IA) Compliance | 26.83% |
| Vulnerability Assessment and Management | 19.81% |
| Knowledge Management | 18.22% |
| Education and Training | 16.69% |
| Data Administration | 16.61% |

- Amongst senior leadership, the greatest need for training was in **Strategic Planning and Policy Development** which was also the area where they spent the most time.
- Participants in the **1811 – Criminal Investigation** series had the greatest need in **Investigation** (65.84%) and **Digital Forensics** (46.12%).

# CONCLUSION

The ITWAC provides a snapshot of the current composition and capabilities of the federal civilian cybersecurity workforce.

- The ITWAC data can serve as a starting point for examining critical skills, determining skill gaps, and identifying training to mitigate gaps.
- It can also illustrate current workforce supply and provide an understanding of the cybersecurity workforce pipeline (e.g., age of the workforce and percentage eligible for retirement).
- Federal departments and agencies can use the data to support strategic cybersecurity workforce development activities such as workforce planning and professional training and development.

- **Key Take-Aways:**
  - The majority of the federal civilian cybersecurity professional population is above the age of 40.
  - While the 2210 occupational series accounts for the largest percentage, cybersecurity professionals are dispersed across other occupational series.
  - Participants from several pay grades and multiple 2210 series parenthetical titles indicated a need for training in **Information Assurance (IA) Compliance**.

# CURRENT ACTIVITIES AND NEXT STEPS

**Current Activities:**

- Prepare the ITWAC Summary Report for official publication.
- Conduct ITWAC POC and Stakeholder engagement to provide ITWAC Reporting Tool support .
- Initiated feedback loop in early February to engage with agency POCs and understand how they are using their ITWAC data at the 30, 60 and 90 day mark.

**Next Steps:**

- Provide findings on National Initiative for Cybersecurity Careers and Studies (NICCS) Portal in March.
- Continue POC and Stakeholder Engagement to provide support regarding ITWAC data analysis and keep them engaged for ITWAC 2014.
- Review feedback survey data to determine how to best improve ITWAC next planned survey (tentative 2014).
- Conduct feasibility study for Non-Federal ITWAC.